

FILED

NOV 14 2014

United States District Court

CLERK, U.S. DISTRICT COURT

DISTRICT OF TEXAS

By

Deputy

In the Matter of the Search of

(Name, address or Brief description of person, property or premises to be searched)

Several electronic items currently in the custody of FBI, located at the Dallas Division, One Justice Way, Dallas, Texas 75220, which are more fully described in Attachment A

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

CASE NUMBER: 3:14-MJ-

**3-14MJ768-BH**

I Christopher Thompson being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation (FBI) and have reason to believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)


(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, concerning a violation of Title 18 United States code, Section(s) 2251(a). The facts to support a finding of Probable Cause are as follows:

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT CHRISTOPHER THOMPSON).

Continued on the attached sheet and made a part hereof. XX Yes    No

  
Signature of Affiant  
CHRISTOPHER THOMPSON  
Special Agent, FBI

Sworn to before me, and subscribed in my presence

November 14, 2014

at

Dallas, Texas

Date

City and State

IRMA C. RAMIREZ

United States Magistrate Judge

Name and Title of Judicial Officer

  
Signature of Judicial Officer

**ATTACHMENT A**  
**Description of Items to be Searched**

1. An Apple iPhone in blue Dallas Cowboys case with assigned telephone number (214) 709-3019;
2. A gray USB metal thumb drive 26B;
3. A T-Mobile Alcatel SPARQ cellular telephone with an 86B SanDisk micro USB;
4. Two (2) Sony digital media players;
5. Samsung model NP365E5C-505US laptop computer;
6. Compaq CQ61-410US laptop computer;
7. Kingston Micro SD 46B;
8. Apple iPad;
9. SIM card 4PSIMC4B;
10. SIM card 8901260662.

These items are currently located at the Federal Bureau of Investigation, Dallas Division, One Justice Way, Dallas, Texas, 75220.

**ATTACHMENT B**  
**LIST OF ITEMS TO BE SEIZED**

All records, documents, data, and information in whatever form that constitute evidence, fruits or instrumentalities of violations of U.S.C. § 2251(a), to include but is not limited to the following:

1. Any file, information, or record indicating the telephone number (214) 709-3019 and/or associated account(s).
2. Any and all correspondence and communications, to include text messaging and voice calls, between telephone number (214) 709-3019 and others.
3. Any and all photographs, visual depictions, records, documents, files, folders, videos, and materials (in whatever form) referencing or otherwise containing the names of associated Facebook/electronic mail accounts maintained and utilized by Cervantes.
4. Any and all files, folders, records, documents, and materials tending to establish the identity of the owner and/or person in control of the Apple iPhone with assigned telephone number (214) 709-3019.
5. Any and all visual depictions of any person under the age of eighteen years old engaging in any sexually explicit conduct as defined in 18 U.S.C. § 2256.
6. Any and all correspondence and communications, to include text messaging and voice mail, concerning violations of 18 U.S.C. § 2422(b) showing persuasion, enticement, or coercion of a minor to engage in criminal sexual activity, or an attempt to do so.
7. Any and all correspondence and communications, to include text messaging and voice mail, concerning the prostitution of children.
8. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other sexually explicit activities with any persons under the age of eighteen years old.
9. Evidence of who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, CHRISTOPHER THOMPSON, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

1. I am submitting this Affidavit in support of an application for a warrant to search the following portable electronic device(s): 1) an Apple iPhone with assigned telephone number (214) 709-3019, 2) a gray USB metal thumb drive, 3) a T-Mobile Alcatel SPARQ cellular telephone with an 8GB SanDisk micro USB, 4) two Sony digital media players, 5) Samsung model NP365E5C-505US laptop computer, 6) Compaq CQ61-410US laptop computer, 7) Kingston Micro SD 4GB, 8) Apple iPad, 9) SIM card 4PSIMC4B, and 10) SIM card 8901260662, belonging to Servando Vega Cervantes. These electronic devices are currently located at the Federal Bureau of Investigation, Dallas Division, One Justice Way, Dallas, Texas, 75220.

**INTRODUCTION**

2. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since April 2004, and I am currently assigned to the Dallas Division. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I am currently assigned to a Child Exploitation Task Force, wherein my duties and responsibilities include investigating criminal violations relating to the sexual exploitation of children (SEOC). I have investigated SEOC violations since 2004 and have gained expertise in these types of investigations through training in

seminars, classes, and my everyday work. In addition, I have received specialized training in the investigation and enforcement of federal child pornography laws in which computers are used as the means for producing, transmitting, collecting and storing child pornography.

4. I am investigating the activities of Servando Vega Cervantes (Cervantes), residing at ## Starlight Drive, Hutchins, Dallas County, TX 75141. As will be show below, there is probable cause to believe that Cervantes knowingly used a person under the age of eighteen years, to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, which were produced using materials that had been mailed, shipped, and transported in interstate and foreign commerce by any means, in violation of 18 U.S.C. § 2251(a).

5. I am submitting this affidavit in support of a search warrant authorizing the search of the following portable electronic device(s): an Apple iPhone, a gray USB metal thumb drive, a T-Mobile Alcatel SPARQ cellular telephone, two Sony digital media players, Samsung laptop computer, Compaq laptop computer, Kingston Micro SD, Apple iPad, and two SIM cards, belonging to Cervantes, and more particularly described in Attachment A, that are currently located at the Dallas Division of the Federal Bureau of Investigation, One Justice Way, Dallas, Texas 75220, for the items specified in Attachment B, constituting instrumentalities and evidence of the foregoing violation.

6. The statements in this affidavit are based on my personal knowledge and experience, as well as on information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of a violation of 18 U.S.C. § 2251(a) will be contained on the electronic devices described above, and belonging to Cervantes.

**BACKGROUND ON COMPUTERS/DIGITAL MEDIA & CHILD  
PORNOGRAPHY**

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, computers, computer technology, other digital electronic storage devices, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

8. Computers and other digital electronic media basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

9. Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable,

or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as Apple iPhones, Apple iPads, e-readers, and tablets now function essentially as computers with the same abilities to store images in digital form.

11. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! Inc., and Google Gmail, among others. The online service(s) allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account(s) from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer or electronic media. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer or other electronic device are often saved or stored on that computer or device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

13. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is



unused after a file has been allocated to a set block of storage space. These types of deleted files can remain in this free or slack space for long periods of time before they are overwritten.

14. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed but more on a particular user's operating system, storage capacity, and computer habits.

15. Because the distribution of child pornography is illegal, child pornography is not readily available through legitimate domestic businesses. However, in contrast, child pornography is widely available via computer or other digital electronic media from individuals who trade such material on the Internet. An individual can use the computer or other digital electronic media in the privacy of his/her own home or office to locate and interact with other individuals offering or seeking such materials. Moreover, an individual can do so without revealing his/her true identity. The use of computers and other digital electronic media devices provide individuals interested in child pornography or obscene images

with a convenient method of storing, organizing, and accessing their collection and information concerning other who collect, trade, or distribute such materials.

16. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following three reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data.
- c. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted

files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

17. The Apple iPhone is a line of smartphones designed and marketed by Apple Incorporated. In addition to functioning as a handheld wireless electronic communication device capable of making and receiving telephone calls, an iPhone can function as a video camera, a camera phone, a portable media player, and an Internet client with email and web browsing capabilities with Wi-Fi and cellular data connectivity. In addition to all of the above capabilities, the Apple iPhone also provides basic functions such as, but not limited to: (1) storing names and phone numbers in electronic "address books;" (2) sending, receiving, and storing text messages and email; (3) taking, sending, receiving, and storing still photographs and moving video; (4) storing and playing back audio files; (5) storing dates, appointments, and other information on personal calendars; (6) accessing and downloading information from the Internet; and (7) receiving, accessing, and storing voice mail.

**ANALYSIS OF ELECTRONIC DATA & SEARCH METHODOLOGY TO  
BE EMPLOYED**

18. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. Surveying various file directories and the individual files they contain;
- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

19. Searching the electronic devices described herein for the evidence described above may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer, or a smart phone, for special words that are likely to appear only in

the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names.

20. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the device's memory not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant.

21. In light of these difficulties, your Affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described above.

### **BACKGROUND OF THE INVESTIGATION**

22. On or about May 20, 2014, the FBI was contacted by the Hutchins Police Department (HPD) regarding questionable online communications between an 11-year-old victim, herein identified as "AP," and the Facebook user profile of "Laura Ortiz" (Ortiz). The victim's mother, herein identified as "AM," believed the user of the Ortiz profile was actually an adult male and not a 13-year-old female as described in the chat conversations between AP and Ortiz.

23. Previously, on or about May 15, 2014, AM reported to the HPD that she allowed AP to maintain a Facebook profile as long as AM was allowed to

regularly review the profile on AP's cellular telephone at any given time. After reviewing AP's profile on this day and reading a chat conversation between AP and Ortiz that AM believed to be of an adult nature, an adult male AM identified as "Jordan" (Jordan) visited her residence and spoke with AP on their porch. AM believed Jordan was using the online profile of Ortiz to deceive her son. AM provided HPD with the password to AP's Facebook profile. HPD requested assistance of the FBI to further investigate this matter.

24. Upon review of AP's Facebook profile with a FBI Language Analyst fluent in Spanish, SA Jennifer Mullican observed a chat conversation between AP, using the Facebook profile of "Jun### H###," and Ortiz which was initiated on May 13, 2014, at approximately 6:48 p.m. At approximately 6:58 p.m., Ortiz asked AP if he would send her a picture of his ".1." but AP did not respond. Later, at approximately 8:42 p.m., AP asked Ortiz, "a picture of my what?" to which Ortiz replied "penis." AP agreed, and at approximately 9:14 p.m., Ortiz replied, "baby, you already have a lot of hairs." The next day, Ortiz requested AP send another image of himself standing or in a mirror. Ortiz subsequently asked AP to send another image "just like that one" but to show his face in the photograph.

25. Subsequently, on or about May 23, 2014, AP was forensically interviewed at the Collin County Children's Advocacy Center in Plano, TX. AP advised he was familiar with Jordan and had met Jordan when AP was visiting a friend's residence in the trailer community where he resides. While at his friend's residence, Jordan told AP about Ortiz and Jordan asked AP for his Facebook

information to provide to Ortiz. Later the same evening, Ortiz sent AP a "friend request" on Facebook and AP accepted the request. AP used the Facebook profile "Jun### H###" because he did not want to use his real name.

26. Also during the interview, AP admitted to sending images of "a body part" and the "front part of his body" to Ortiz, however AP would not identify the body part as his genitalia. AP advised he deleted the images from his cellular telephone so his mother would not find the images when she looked at his phone.

27. Later, on or about October 31, 2014, AM advised the HPD that she believed Jordan was now living in the trailer community and that AM could point out his residence and his vehicle. HPD met with AM and AM pointed out a black, 4-door Acura, Texas license plate "DR###62" she believed to be owned and driven by Jordan. Database records showed this vehicle to be registered to Cervantes at ## Starlight Drive, Hutchins, TX.

28. On or about November 12, 2014, HPD, SA Jennifer Mullican and other law enforcement personnel established surveillance in close proximity to ## Starlight Drive, Hutchins, TX. The black Acura driven by Cervantes was observed by HPD parked in the parking stalls located in front of the residence. The vehicle subsequently departed the location, and HPD initiated a traffic stop for failure to signal a lane change and for window tint that was too dark. Cervantes was the lone occupant of the vehicle, and he was observed operating a motor vehicle without a license. Cervantes was transported to the HPD and placed in a holding cell.

29. After being processed by HPD, Cervantes was interviewed by Special Agent Miguel Torres. Cervantes admitted to SA Torres that he is the user of the Ortiz Facebook profile, and he knows AP on Facebook as "Junior." Cervantes told SA Torres he used the Ortiz account to convince AP to allow Cervantes to teach AP to masturbate. Cervantes reviewed the printed chat conversation between Ortiz and AP and Cervantes acknowledged it was he who engaged in this conversation with AP. Cervantes told SA Torres he understands that trying to entice minors online is illegal, and he believed that inappropriate images of AP would be found on his cellular telephone.

30. Furthermore, Cervantes advised SA Torres that he met with and taught AP how to masturbate while sitting in his vehicle in front of the mailboxes at his residence. Cervantes stated he touched AP's genitals as AP masturbated and Cervantes took photographs of AP while AP masturbated. Cervantes described AP as erect when Cervantes touched AP's genitals. Cervantes believed these photographs would be observed on his Apple iPhone cellular telephone.

31. Additionally, AM reviewed Cervantes' booking photograph and confirmed Cervantes was Jordan and Cervantes was the individual who met and talked with AP on their front porch.

32. Cervantes provided agents with written consent to examine his Apple iPhone cellular telephone. A forensic preview of Cervantes' cellular telephone was conducted on scene, and images of prepubescent males were observed on the device. Cervantes advised images and videos of additional



victims would be discovered on his cellular telephone, however he could not recall the identities of these victims without accessing his telephone.

33. Furthermore, Cervantes advised that electronic devices containing images and videos of child pornography would be located in his bedroom at ## Starlight Drive, Hutchins, TX. One device, identified by Cervantes as a thumb drive, was hidden in a location that Cervantes had trouble describing to investigators. Cervantes offered to take agents to his residence to point out the electronic devices that stored child pornography.

34. Subsequently, Cervantes, transported by SA Christopher W. Thompson and others, went to ## Starlight Drive, Hutchins, TX. SA Thompson and other law enforcement personnel, upon obtaining written consent, searched Cervantes' bedroom for electronic devices identified by Cervantes as containing child pornography.

35. Cervantes identified the following devices in his bedroom as likely or definitely containing images of sexual exploitation of minor victims: a gray USB metal thumb drive, a T-Mobile Alcatel SPARQ cellular telephone with an 86B SanDisk micro USB and a Samsung model NP365E5C-505US laptop computer. Cervantes could not recall specifically but stated the following could contain records of contacts with minors or images of the sexual exploitation of minor victims: two Sony digital media players, a Compaq CQ61-410US laptop computer, a Kingston Micro SD 46B, an Apple iPad, a SIM card 4PSIMC4B, and a SIM card 8901260662.

36. Cervantes offered to identify persons in some of the images known to be stored on the gray USB metal thumb drive. Cervantes granted consent to search this thumb drive and SA Thompson forensically reviewed the contents of this thumb drive with Cervantes. Cervantes identified at least five videos taken of a minor hereafter identified as "R". Cervantes believes R is fourteen years old. R was sleeping in Cervantes's bedroom and Cervantes pulled down R's shorts and underwear exposing his genitals. Cervantes touched R's penis in the videos and put his mouth on R's penis in one of the videos. Cervantes identified other videos of a minor hereafter referred to as "C". Cervantes believes C is seventeen years old. With his cellular phone, Cervantes filmed C masturbating in Cervantes's bathroom. Cervantes copied these videos from his phone to this gray USB thumb drive.

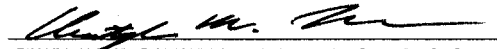
#### CONCLUSION

37. In conclusion, I believe that there is probable cause to believe that Cervantes used the Apple iPhone and other personal electronic devices to knowingly use a person under the age of eighteen years, to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, which were produced using materials that had been mailed, shipped, and transported in interstate and foreign commerce by any means, in violation of 18 U.S.C. § 2251(a).

38. Therefore, based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the Apple iPhone

and other personal electronic devices belonging to Cervantes, more particularly described in Attachment A, is evidence and an instrumentality of violations of 18 U.S.C. § 2251(a), and that evidence of those offenses, more particularly described in Attachment B to this affidavit, will be found on these devices.

39. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the electronic devices listed in Attachment A and the seizure of the items listed in Attachment B.

  
CHRISTOPHER W. THOMPSON  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me this 14<sup>th</sup> day of November, 2014.

  
IRMA CARRILLO RAMIREZ  
UNITED STATES MAGISTRATE JUDGE